VMware vCenter Server
多个漏洞通告

2021 年 9 月 28 日

目录

一、 漏洞概要

漏洞名称	VMware vCenter Server 多个漏洞
影响组件	VMware vCenter Server
影响范围	VMware vCenter Server 7.0 VMware vCenter Server 6.7
漏洞类型	文件上传
利用条件	通过访问 443 端口可直接利用
综合评价	<综合评定利用难度>：容易，无需授权即可远程代码执行。 <综合评定威胁等级>：高危，能造成远程代码执行。

二、 漏洞分析

2.1 组件介绍

VMware vCenter Server 是美国威睿（VMware）公司的一套服务器和虚拟化管理软件。该软件提供了一个用于管理 VMware vSphere 环境的集中式平台，可自动实施和交付虚拟基础架构。

2.2 漏洞描述

2021 年 9 月 22 日，深信服安全团队监测到一则 VMware 官方发布安全补丁的通告，共修复了 19 个安全漏洞，其中包含 1 个严重漏洞的信息。

VMware vCenter Server 文件上传漏洞 CVE-2021-22005。VMware vCenter Server 的分析服务中存在一个任意文件上传漏洞。可以访问 443 端口的恶意行为者可能会利用此漏洞，通过上传特定文件在 vCenter Server 上执行代码。

序号	漏洞名	漏洞编号	严重等级	影响版本
1	VMware vCenter Server 文件上传漏洞	CVE-2021-22005	严重	VMware vCenter Server 7.0 VMware vCenter Server 6.7
2	VMware vCenter Server 反向代理绕过漏洞	CVE-2021-22006	高危	
3	VMware vCenter Server 本地信息泄漏漏洞	CVE-2021-22007	中危	
4	VMware vCenter Server VPXD 拒绝服务漏洞	CVE-2021-22010	中危	
5	VMware vCenter Server 分析服务拒绝服务漏洞	CVE-2021-22020	中危	

6	VMware vCenter Server 本地权限提升漏洞	CVE-2021-21991	高危	

三、 影响范围

可能受漏洞影响的资产广泛分布于世界各地，国内省份中受影响资产分布于广东、江苏、浙江等省市。

目前受影响的 **VMware vCenter Server** 版本：

VMware vCenter Server 7.0

VMware vCenter Server 6.7

VMware vCenter Server 6.5

四、 解决方案

4.1、官方解决方案

当前官方已发布受影响版本的对应补丁，建议受影响的用户及时更新官方的安全补丁。链接如下：

https://www.vmware.com/security/advisories/VMSA-2021-0020.html

4.2、如何检测组件系统版本

登录 VMware vCenter Server 后，在主机页面中即可查看相应的版本信息。